IT Security Procedural Guide: Conducting Penetration Test Exercises
CIO-IT Security-11-51

Revision 5

July 27, 2020

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Revision 1 – April 30, 2012		
1	Bo Berlas	Clarified guidance relating to performance of penetration testing against development environments.	Penetration testing shall occur against production environments to ensure testing activities reflect the risks of the system under review.	8
		Revision 2 – December 11, 2014		
1	Bo Berlas	Changed requirement for penetration testing from ALL systems (i.e., FIPS PUB 199 Low, Moderate and High) to FIPS PUB 199 Low and Moderate Internet accessible systems and All FIPS PUB 199 High.	Focuses penetration testing activities at areas of greatest risk. Aligns with updated requirements in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk".	Pages 4 and 8
2	Bo Berlas	Changed references to Office of the Senior Agency Information Security Officer (OSAISO) and Senior Agency Information Security Officer (SAISO) to Office of the Chief Information Security Officer (OCISO) and Chief Information Security Officer (CISO)	Administrative to reflect changes in office name and CISO title as a result of IT and IT Security consolidation.	Numerous
3	Blanche Heard	Updated to reflect references to comply with ADM O 5440.667	Organization titles and responsibilities	Numerous
		Revision 3 – December 1, 2015		
1	Bo Berlas	Updated Reporting Template and associated references	Updated to reflect changes to NIST SP 800-53 Rev 4 and reflect process updates	Pages 9 and 20
2	William Salamon	Updated Reporting Template, Rules of Engagement Template, and updated several sections	Reflect changes to OWASP, NIST SP 800-15 recommendations, incorporate cloud computing concepts, and other process updates	Pages 11-12, 16-17, 21-22
		Revision 4 – January 18, 2018		
1	Dean/ Feliksa/ Klemens/ Newsome	Revised to reflect current GSA processes and procedures for conducting penetration tests.	Revised to reflect how GSA conducts penetration tests based on Federal policies, NIST controls with GSA parameters, and GSA processes and procedures. Updated to current guide structure and format.	Throughout
		Revision 17 – July 27, 2020		
1	Armando Quintananieves/Angela Christian/ Raja Hayat/ Branndon Dean	Primary changes: • Expanded the types of pen tests listed • Clarified pen test approaches	Revised to reflect current GSA processes and procedures for conducting penetration tests in different environments.	Throughout

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		• Added section on specific pen tests GSA conducts and their applicability • Added section on responsibilities for system and pen test roles • Added an Appendix with GSA A&A Penetration Test Minimum Requirements • Modified formatting and style to latest guidance, including 508 compliance		

Approval

IT Security Procedural Guide: Conducting Penetration Test Exercises, CIO-IT Security 11-51, Revision 5, is hereby approved for distribution.

X DocuSigned by:
Bo Berlas
FD717926161544F...

Bo Berlas
GSA Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division (ISP) at ispcompliance@gsa.gov.

Table of Contents

1 Introduction 1
1.1 Purpose 1
1.2 Scope 1
1.3 Policy 1
1.4 References 2

2 Penetration Testing Overview 2
2.1 Penetration Testing Approaches 5
2.2 Defining the Scope and Test Boundary 7
2.3 Vulnerability Risk Rating 7
2.4 Exploiting Vulnerabilities 7

3 GSA Penetration Tests Defined 8
3.1 GSA A&A Penetration Test: 8
3.1.1 Web Application Penetration Tests: 8
3.1.2 Network Penetration Tests: 8
3.2 GSA Annual Penetration Test: 8
3.2.1 FIPS Moderate and Low 8
3.2.2 FIPS High 8
3.2.3 FISMA High Value Assets (HVAs) 8
3.2.4 Ongoing Authorization (OA) 9
3.3 GSA Delta Penetration Test 9
3.4 GSA Incident Response (IR) Penetration Test 9

4 GSA Penetration Testing Process 9
4.1 Responsibilities 10
4.1.1 ISSM/ISSO 10
4.1.2 Pentest Lead 10
4.1.3 System Owner 10
4.1.4 Penetration Tester/Team 10
4.2 Planning Phase 10
4.2.1 Penetration Test Scope 11
4.3 Defining the Rules of Engagement 12
4.4 Penetration Testing Authorization 13
4.5 Test Phases 13
4.6 Additional Considerations 14

5 Incident Response Procedures 15

6 Points of Contact 15

Appendix A: Pentest Minimum Requirements Matrix 16

Appendix B: Conducting Penetration Test Templates 17

Appendix C: GSA A&A Penetration Test Detailed Min Requirements (Including HVA A&A and Annual Penetration Testing) 18

Table A-1: Pentest Minimum Requirements Matrix 16

Notes:

- Hyperlinks in running text will be provided if they link to a location within this document (i.e., a different section or an appendix). Hyperlinks will be provided for external sources unless the hyperlink is to a webpage or document listed in Section 1.4. For example, Google Forms, Google Docs, and websites will have links.
- It may be necessary to copy and paste hyperlinks in this document (Right-Click, Select Copy Hyperlink) directly into a web browser rather than using Ctrl-Click to access them within the document.

1 Introduction

A penetration test is an authorized simulation of a cyber-attack which is used to identify security weaknesses by way of technical flaws, misconfigurations, software vulnerabilities, and/or business logic. A penetration tester will attempt to exploit weaknesses to gain access, modify functionality, and/or corrupt the business logic of the target system without creating additional risk to the agency or organization. The penetration tester will attempt to perform activities of a malicious actor; however, such activities will be conducted ethically and with the permission of the General Services Administration (GSA) Office of the Chief Information Security Officer (OCISO) prior to execution.

A penetration test exercise supports the overall security process by identifying security risks and demonstrating exploitability of findings that may not be readily apparent when performing a security review. A penetration test can be performed with or without knowledge of the system, and involves the execution of a scenario and abuse cases that focus on violating technical, administrative, and management controls to gain access to the system or data.

Penetration tests can be used to verify and prove scan results that are false positives or false negatives. Penetration tests, as opposed to vulnerability scans, should not have false positive findings since they report only on found vulnerabilities. Penetration tests while capable of verifying or proving a specific false negative finding, are not exhaustive and therefore cannot prove there are no vulnerabilities to a system. The test processes described in this document are used for measuring, evaluating, and testing the security posture of an information system, but test findings should not be used to the exclusion of other security processes (e.g., architecture analyses, configuration checks.)

1.1 Purpose

This procedural guide provides guidance for performing penetration test exercises against GSA applications, infrastructure, and systems. It provides GSA associates and contractors with significant security responsibilities as identified in the current Chief Information Officer (CIO) GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy,*" and other IT personnel involved in penetration testing exercises on GSA IT resources, an independent repeatable framework for conducting penetration test activities.

1.2 Scope

The requirements outlined within this guide apply to any internal or external organizations who are involved in penetration testing of GSA information systems and data.

1.3 Policy

Penetration testing is addressed in CIO 2100.1 as stated in the following paragraphs:

Chapter 3, Paragraph 4:

> *b. All Internet accessible information systems, and all FIPS 199 High impact information systems are required to complete an independent penetration test (or 'pentest') and provide a Penetration Test Report documenting the results of the exercise as part of the A&A package. In addition, these same systems must complete penetration tests annually. The annual penetration tests can be completed internally and do not require an independent assessor.*
>
> *c. Independent vulnerability testing including penetration testing and system or port scanning conducted by a third-party such as the GAO and other external organizations must be specifically authorized by the AO and supervised by the ISSM.*

1.4 References

Federal Standards and Guidance:

- Federal Information Processing Standards (FIPS) Publication 199, "*Standards for Security Categorization of Federal Information and Information Systems"*
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-115, "*Technical Guide to Information Security Testing and Assessment"*
- NIST SP 800-145, "*The NIST Definition of Cloud Computing*"
- National Vulnerability Database (NVD) Common Vulnerability Scoring System (CVSS) Support, "*The Common Vulnerability Scoring System"*

GSA Directives, Policies, and Procedures:

- GSA CIO Order 2100.1, "*GSA Information Technology (IT) Security Policy"*
- CIO-IT Security-01-02, "*Incident Response*"

Other Applicable Sources:

- Open Web Application Security Project (OWASP) Testing Guide 4.1, "*OWASP Testing Guide*"
- PTES, "*Penetration Testing Execution Standard*"
- PTES-TG, "*Penetration Testing Execution Standard Technical Guidelines*
- SANS TOP 25, "CWE/SANS TOP 25 Most Dangerous Software Errors"
- Common Vulnerability Scoring System (CVSS) v3.x
- OWASP Serverless Top 10
- OWASP Top 10

2 Penetration Testing Overview

A penetration test is an authorized simulation of a cyber-attack which is used to identify security weaknesses by way of technical flaws, misconfigurations, software vulnerabilities, and/or business logic, with or without knowing the inner workings of the system. NIST SP 800-115 describes two primary viewpoints; external and internal testing.

External security testing offers the ability to view the environment's security posture as it appears outside the security perimeter—usually as seen from the Internet—with the goal of revealing vulnerabilities that could be exploited by an external attacker.

In internal security testing, assessors work within the security perimeter, assuming the identity of a trusted insider or an attacker who has penetrated the perimeter defenses. This kind of testing can reveal vulnerabilities that could be exploited and demonstrates the potential risk to the organization or agency. Internal security testing also focuses on system-level security and configurations including application and service configuration, authentication, access control, and system hardening.

In general, there are fourteen types of penetration tests:

Network Penetration Tests:

Network penetration tests are used to evaluate the susceptibility of information systems to network attacks by identifying and exploiting weaknesses found in networks, hosts, and devices to help assess the level of risk posed by specific vulnerabilities in accordance with PTES and PTES-TG.

Web Application Penetration Tests:

Web application security testing is focused on evaluating the security of a web application. The process involves an active analysis and exploitation of the web application for any weaknesses, technical flaws, or vulnerabilities in accordance with the OWASP Testing Guide 4.1.

Software or Application Penetration Tests (including Mobile Applications, and API):

Software application testing is focused on evaluating the security of internal software applications. White box testing is generally used during the developmental phase to find and remediate system flaws in the application prior to deployment. Software testing generally utilizes reverse engineering and its techniques.

Social Engineering Tests:

Social engineering testing is focused on evaluating the human aspect of the organization or agency. Social engineering testing is a way to test the organizational security awareness training program through means such as email phishing or other social or non-technical means.

Wireless Network Penetration Tests:

Wireless network penetration tests are used to evaluate the susceptibility of the Agency's wireless information network. This pentest focuses on wireless network components, including but not limited to access points, Internet of Things (IoTs), and hosts. It helps to assess the level of risk posed by specific vulnerabilities in accordance with PTES and PTES-TG.

Physical Penetration Test:

The primary objective for a physical penetration test is to measure the strength of existing physical security controls and uncover their weaknesses before bad actors are able to discover and exploit them.

Physical penetration testing, or physical intrusion testing, will reveal real-world opportunities for malicious insiders or bad actors to be able to compromise physical barriers (i.e.: locks, sensors, cameras, mantraps) in such a way that allows for unauthorized physical access to sensitive areas leading up to data breaches and system/network compromise.

Incident Response Penetration Test:

Test performed at the request of the Incident Response Federal Lead or Information Security (IS) Division Directors with approval from GSA CISO in response to an identified incident on an external facing Web Application. Incident response penetration tests utilize SANS TOP 25 and can be either authenticated or unauthenticated. The test can include specific exploits that were observed during the incident. Additionally, internal testing may be done to determine the extent of the incident.

Phishing:

Phishing testing is performed regularly agency wide by the Security Operations Division (SecOps). GSA currently uses CoFense but any other tool can be used. Phishing emails are sent to randomly selected GSA federal employees and contractors. By request from the associated Federal Information Security Management Act (FISMA) systems the Information System Security Manager (ISSM)/Information System Security Officer (ISSO) or GSA CISO, a phishing attack can be designed and carried out on any provided end users and admin role GSA users. At the end of the attack a report will be provided demonstrating the success of the attack identifying users who were successfully phished.

Network Stress Testing:

Stress testing is a procedure to find out whether a computer, application, device or the entire network can withstand high loads and remain operational. A stress test can be a simulation of an adverse condition that takes a system down or at least decreases its performance. These types of tests are recommended for any component on the GSA network. This type of test is not recommended for any Amazon Web Services (AWS) component without prior AWS approval.

Cloud Penetration Testing:

The type of penetration tests take place in the cloud environment, during this process the penetration tester will review cloud security configurations as well as systems, web apps and another component associated with the cloud environment.

Serverless Penetration Testing:

Applications that run on serverless providers such as AWS lambda and Google Cloud Functions use this form of penetration testing focusing on new perspectives and vulnerabilities from a Serverless environment such as Hypertext Transfer Protocol (HTTP) Application Programming Interfaces (APIs), messages, cloud storage, and IoT devices, including protocols used for these components. Taking into consideration the attack surface complexity, and overall system complexity, testing is performed based off of OWASP Serverless Top 10.

Red Team/Blue Team (Purple Team) Testing:

Purple teaming is a security methodology whereby red and blue teams work closely together to maximize cyber capabilities through continuous feedback and knowledge transfer.

OSINT Assessment:

Open-source intelligence (OSINT) is a highly diverse form of intelligence collection and analysis of data collected from overt and covert sources to be used in an intelligence context by the executives to make proactive decisions based on imminent risks facing the organization at a tactical and strategic level.

OSINT assessment may include active scanning for sensitive domain data on darknet as well as listening for darknet chatter of upcoming attacks which will assist executives in long term strategic decision making. OSINT may also include passive techniques including using web crawlers such google search indexing engine to identify accidental data/vulnerability exposure on the internet as well as organizational threat discussions on social media.

Business Logic Assessment:

Business Logic Assessments (BLAs) are manual assessments of application security weaknesses that cannot be tested effectively in an automated manner. BLA's consist of reviewing internal policies and procedures and applying those to an application's business logic to identify and limit risk factors to the Agency.

2.1 Penetration Testing Approaches

As part of planning the penetration test exercise, the test team has to determine what level of access will be required for the exercise. The penetration tester acts like an attacker and attempts to find and exploit vulnerabilities within the defined scope and boundaries granted by the Rules of Engagement. In many cases, the penetration tester will be given a valid account on the system. There are often different terms used to describe these perspectives, which include: black box, gray box, and white box testing as defined below.

Black Box Testing:

The black box testing approach assumes no knowledge of the internal structure and implementation detail of the assessment object. Because an attacker will incorporate a low and slow attack strategy to avoid detection of the targeted attack, this approach can take months and even years to gain enough information about the system to initiate an effective cyber-attack.

Black box testing is very difficult to simulate as most penetration tests typically only last a few weeks. This type of testing is only done with CISO approval.

At a minimum the following information will be provided to the penetration testing team:

- Network Diagram
- IP/FQDN

White Box Testing:

In white box testing, the penetration tester has full unrestricted access to the target environment as well as the internal structure and source code. It can include running test cases to check whether the system meets specification requirements. Using derived test cases, the user exercises the test cases by providing input to the system and comparing the actual output to expected output. In this type of testing, the user has to go beyond the user interface to test the correctness of the system. The white box testing approach is typically used by developers to find weaknesses in the system.

White box testing is one of the best approaches to find errors in the development stage of the life cycle. In this process, deriving test cases is an important part of the test exercise. The test case design strategy should include execution of all lines of the source code and/or all available functions at least once to complete 100% code coverage during testing. Access to underline documents, network, and all levels of access will be required. This type of testing is only done with IS Director or CISO approval.

At a minimum the following information will be provided to the penetration testing team:

- Network Diagram
- System Security Plan (SSP)
- Full Admin Level to internal and external interface
- List of Administrator users to both Network and Web interface
- Vulnerability Scan Data (Web/Network/Software)
- Code Coverage
    - Control Flow Testing
    - Data Flow Testing
    - Branch Testing
    - Statement Testing
    - Decision Coverage
    - Modified condition/decision Coverage
    - Prime Path Testing
    - Path Testing

Gray Box Testing: (GSA's Accepted Pentest Standard)

Gray box testing is a hybrid approach between black box and white box testing. In gray box testing, the internal structure is partially known. This often involves having access to internal data structures and algorithms for purposes of designing the test cases, but testing at the user, or black box level. Gray box testing provides many of the benefits of white box testing such as reducing the time required for information gathering while maintaining the external threat perspective.

At a minimum the following information will be provided to the penetration testing team:

- Network Diagram
- SSP
- Accounts (Web Interface/Network) - One of each role
- List of Administrator users to both Network and Web interface

- Vulnerability Scan Data (Web/Network/Software)

There are multiple factors to consider when deciding which approach to use on a target system. It is important to remember the relationship between time and system exposure. While time is a restraint to ethical hackers (white hats), system exposure comes as a restraint to the non-ethical hackers (black hats). Utilizing the gray box testing approach allows white hats to save time by working with developers and system administrators to understand the functionality and operation of target systems while a black hat would have to spend more time researching the system in an attempt to gain similar knowledge.

2.2 Defining the Scope and Test Boundary

Properly defining the scope of the penetration test is necessary to ensure the test exercise is focused on relevant components and to safeguard against testing components that are outside of the authorized system boundary. ISSM/ISSO's and test personnel must strike a balance between performing a comprehensive set of tests and evaluating functionality and features that present the greatest risk. Any special cases or sensitivities should be carefully evaluated to prevent disruption of service prior to the start of the exercise. GSA's accepted standard scope is any interaction that is identified in the SSP, any testing of interconnections with third party entities is considered out of scope until the third party agrees to an assessment.

2.3 Vulnerability Risk Rating

Risk ratings provide GSA with a metric to calculate the associated risk of an identified vulnerability. Risk ratings are defined by the NIST CVSSv3.x based score. These risk ratings are used by the penetration tester to justify the assigned severities of vulnerabilities. A penetration tester will typically use the CVSSv3.x calculation:

Attack Vector (AV): Attack Complexity (AC): Privileges Required (PR): User Interaction (UI): Scope (S): Confidentiality (C): Integrity (I): Availability (A)

For additional information see reference in Section 1.4.

Note: Vulnerability Severity can deviate from NIST CVSSv3.x when directed by GSA SecOps management. For example, vulnerabilities associated with Binding Operational Directive (BOD) compliance have an elevated Severity. While findings with risk mitigation implemented may have a decreased severity rating to account for risk mitigation.

2.4 Exploiting Vulnerabilities

The purpose of a penetration test is to identify risk to GSA by exploitation of potential vulnerabilities and/or other security weaknesses. Because security scan tools do not always validate the presence of a finding, scanning tools are often configured to make educated guesses about the presence of potential vulnerabilities, and in certain cases, validation requires a human to perform manual inspection and testing to confirm the finding. Actively exploiting a system is often much harder than simply identifying potential vulnerabilities. A penetration tester will utilize various open source and commercial pentesting tools through its engagement.

While the specific means and methods used to exploit vulnerabilities may vary, Section 3 defines the process which will be applied to ensure test activities are reasonable and conducted within appropriate limits.

3 GSA Penetration Tests Defined

3.1 GSA Assessment and Authorization (A&A) Penetration Test:

3.1.1 Web Application Penetration Tests:

The GSA A&A Web Application Penetration Test is for external only systems. This penetration test is gray box (unless otherwise specified with the appropriate approvals), authenticated and covers all OWASPv4.1 controls. All external facing FISMA systems involved in the full A&A process require a GSA A&A penetration test. A request for an internal Web Application Penetration Test system will require approval from the ISSM, IS Directors, or GSA CISO. Penetration testing of all environments (Test/Dev/Prod) will only be allowed with approval of the IS Federal Penetration Tester Lead.

3.1.2 Network Penetration Tests:

The GSA A&A Network Penetration test is for any FISMA system with external facing components or lacks an external presence. During this pentest the network side is penetration tested using PTES-TG and any web applications are penetration tested using OWASPv4.1 controls. Network Penetration testing can be performed from an internal or external perspective depending on the needs of the network and what is defined as the scope within the SSP. These penetration tests are authenticated and gray box unless otherwise specified with the appropriate approval. Penetration testing of all environments (Test/Dev/Prod) will only be allowed with approval of the IS Federal Penetration Tester Lead.

3.2 GSA Annual Penetration Test:

3.2.1 FIPS Moderate and Low

GSA's annual penetration test is performed on external only interfaces. These penetration tests are unauthenticated and at a minimum shall utilize OWASP's Top 10 and performed on a sampling of GSA hosted Web Applications based on FIPS 199 security categorization level, and on FISMA systems that did not have a full A&A pentest or annual pentest in the last 12 months. Annual penetration tests do not qualify for submission with the A&A Package. Only the penetration tests described above under GSA A&A Penetration tests qualify. Annual penetration testing does not replace the GSA A&A Penetration Test requirement.

3.2.2 FIPS 199 High Systems

FIPS 199 High systems are required to have yearly annual penetration testing.

3.2.3 FISMA High Value Assets (HVAs)

All FISMA HVAs require annual OWASPv4.1 and Network PTES-TG penetration testing.

3.2.4 Ongoing Authorization (OA)

Systems in OA receive an annual penetration test based on the FIPS 199 security categorization level as described above. Any exceptions to this rule will need ISO Director or CISO approval.

3.3 GSA Delta Penetration Test

GSA's Delta penetration test is geared towards penetration testing minor changes to a web application. Delta penetration tests are authenticated, utilize OWASP and gray box. The scope is defined by the changes made to the application only. Delta penetration tests are only conducted with approval from the FISMA system ISSM/ISSO. Penetration testing of all environments (Test/Dev/Prod) will only be allowed with approval of the IS Federal Penetration Tester Lead.

3.4 GSA Incident Response (IR) Penetration Test

GSA's IR Penetration test is conducted with CISO approval and in response to a documented incident. Incident response penetration tests can be either unauthenticated or authenticated, are gray box and utilizes SANs Top 25 Web Application Vulnerabilities testing methodology.

Note: All GSA Penetration tests must be performed against the production environment. If the system is a new system the system will need to be placed into "pre-prod". Test and Dev environments are not externally accessible. Any requests to pentest outside of the production or pre-production environment must be submitted by the ISSM and approved by CISO. This approval will then be documented and included the penetration teams' final package. Penetration testing of all environments (Test/Dev/Prod) will only be allowed with approval of the IS Federal Penetration Tester Lead.

4 GSA Penetration Testing Process

GSA requires an independent penetration on the information system or system components for all Internet facing and FIPS 199 High information systems.

Independent penetration agents or teams are individuals or groups who conduct impartial penetration testing of organizational information systems. Impartiality implies that penetration agents or teams are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the information system(s) that are targeted by the penetration testing exercise.

The following sections constitute a generic version of the penetration test process to be followed for network, software/application, and web application penetration testing. The test phases may be repeated as required through the process based on the scope of the exercise.

4.1 Responsibilities

A Penetration Test is a coordinated effort between the ISSM/ISSO, Systems Owner and the Penetration Testing team. The following lists the responsibilities of each party in conducting a penetration test.

4.1.1 ISSM/ISSO

- Initiates the penetration test request with Pentest Lead
- Provides the type of penetration test to be conducted
- Identifies Scope/Provides SSP
- Signs the Rules of Engagement (RoE)

Note: Penetration tests that fall outside of the accepted GSA standard will be addressed with ISO Federal and Contractor leadership.

4.1.2 Pentest Lead

- Drafts Kick Off meeting slides and RoE
- Schedules Kick Off meeting
- Verifies the Penetration Test Type
- Validates the Scope
- Manages the Penetration Test schedule
- Assigns a Penetration tester
- Signs the RoE
- Circulates the RoE for signatures.

4.1.3 System Owner

- Conducts System Backups
- Provide Pentester Access
- Provides an acceptable penetration test window.
- Whitelists the Pentest VPN
- Signs the RoE

4.1.4 Penetration Tester/Team

- Conduct the penetration test
- Provide risk rating and recommendation
- Validating remediation
- Signs the RoE

4.2 Planning Phase

A kickoff meeting must be held to share contact information and establish key points of the project timeline. The kickoff meeting typically covers the following topics.

- Key personnel points of contact

- Review Rules of Engagement Document
- Define responsibilities in accordance with the Pre-Engagement Checklist
    - Conduct a manual non-intrusive review of any relevant forms, queries, previous vulnerability and/or penetration test reports
- Testing window start and finish times and dates
- Review final reporting process
- Signed final Rules of Engagement Document via Electronic Signature

The kickoff meeting should include the Penetration Testing Program Manager, System/Program Managers, and Lead Penetration Tester. Key stakeholder(s) should be fully aware of the test protocol, and be able to intervene when necessary.

Note: System Owners are responsible for backing up their systems prior to the start of testing. In addition, organizations may also want to have their continuity of operations and disaster recovery plans in place and operational prior to testing so they are assured that system failures due to testing can be quickly and efficiently overcome.

Note: A Kickoff Meeting Presentation Template is available on the GSA InSite IT Security Forms and Aids webpage. Google Doc versions of all Penetration Testing templates are available for internal team penetration tests on Google Drive.

Prior to signing the Penetration Test Authorization Memorandum (IT Security Forms and Aids), System Owners are responsible for notifying all third parties that will be affected by the Penetration Testing exercise which includes but is not limited to:

- Cloud Services Provider(s);
- Internet Service Provider(s); and/or
- Other System Owners using the same platform.

For any external penetration testing, the Penetration Testing Team is responsible for obtaining a signed Penetration Test Authorization Memorandum from GSA as proof of authorization regarding any penetration testing exercises on GSA systems and data and providing it to their Internet Service Provider (as necessary). Even though the client may approve this risk, it must always be clearly communicated with the Internet Service Provider.

Note: Any documentation provided to the Internet Service Provider must first be cleared by the GSA OCISO.

4.2.1 Penetration Test Scope

The Penetration Test scope defines what is being tested. For all penetration tests the scope must be defined and provided to the penetration testing team by the ISSM/ISSO. For A&A Assessments, the scope provided should match the boundaries defined in the SSP. If an SSP is not available, the penetration testing team will work with the ISSM/ISSO and System Owner to outline and validate the scope of the penetration test. The scope will be reviewed and identified in the RoE.

4.3 Defining the Rules of Engagement

Penetration testing is used to identify security weaknesses by way of technical flaws, misconfigurations, software vulnerabilities, and/or business logic. In order to minimize the potential for service disruption, damage, or loss of integrity, the OCISO IST Division provides a Penetration Test Rules of Engagement Template (IT Security Forms and Aids) which outlines the responsibilities and limitations of the testing team and the system owner throughout the entire testing process. Prior to testing, the Authorization Memorandum template must be completed and signed by key personnel in order to ensure there is a common understanding of the limitations, constraints, liabilities, and considerations between the System Owner and the Penetration Testing Team throughout the GSA penetration test process.

During this process, stakeholder(s) should establish specific reporting thresholds in a manner consistent with the risk and impact of any potential vulnerability. OCISO IST Division recommends that thresholds be established in a manner that allows the Penetration Tester to determine the impact of vulnerability exploitation, not just the existence or presence of vulnerabilities. Knowing the potential impact and severity of individual flaws will allow developers and engineers to focus efforts on patching and fixing vulnerabilities based on their severity levels.

If the Penetration Testing Team identifies a high-risk vulnerability, the finding will be reported to the ISSO, ISSM, and System Owner. As part of this notification, the System Owner agrees to not modify the system until the end of the assessment or approval from the Penetration Testing Team. The Penetration Testing Team will work with the System Owner upon remediation(s) to validate vulnerability findings have been resolved.

In general, the execution of a penetration test exercise involves the active exploitation of systems and information. While the objective of the penetration test is to recreate the conditions and environment that can be exploited by a bad actor, a GSA-sanctioned penetration test is a scenario designed to explore existing vulnerabilities in a controlled and deliberate manner.

Important principles of GSA penetration test exercises include but are not limited to:

- The Penetration Testing Team will not violate the scope or boundary of the Penetration Testing Exercise defined in the Rules of Engagement and the Authorization Memorandum.
- The Penetration Testing Team will not maintain persistence beyond the testing window defined in the Authorization Memorandum.
- The Penetration Testing Team will not introduce any new vulnerabilities to the target system or its components.
- The Penetration Testing Team will not modify, or delete log/audit trails of a target system to clear their tracks.

Prior to testing, all personnel involved should have a common understanding of the limitations, constraints, liabilities, and indemnification considerations between the System Owner and the assessment team throughout the penetration test. The Penetration Testing Team may attack the application which may disable account users or system services. In the case of any service interruptions, the System Owner will be responsible for resetting accounts in a timely manner so as not to restrict or extend the testing window.

4.4 Penetration Testing Authorization

Prior to commencement of penetration test activities, OCISO must review the Rules of Engagement document and approve the Authorization Memorandum. Upon approval of the Authorization Memorandum, permission will be granted specific members in the Penetration Testing Team to conduct penetration tests against GSA's assets defined in the applicable SSP while conducting such test(s) in accordance with the rules defined in the project Rules of Engagement Document.

4.5 Test Phases

The testing process will involve four primary phases: information gathering (mapping/ reconnaissance), discovery, exploitation (attack) and documentation/reporting. After performing the necessary notifications, the Penetration Testing Team will begin information gathering activities. The purpose of the information gathering phase is to collect any data that can be used as inputs for discovering vulnerabilities. The testing phases may be repeated multiple times throughout the exercise (as required) based on the Rules of Engagement and structure of the tests assigned to the exercise.

The information gathered during the mapping/reconnaissance phase is reviewed to mark potential exploitable vulnerabilities. Information gathering is critical to understanding the attack surface and establishing the system's public footprint which include:

- Discovering open source disclosures
- Enumerating public interfaces
- Identifying system architecture and components
- Diagramming application flow and design
- Surveying the hosting environment
- Discovering control channels

Vulnerability discovery is the process of testing and probing system entry points for flaws that can be used to generate an error condition, raise an invalid response, monitor traffic or data, or control a key system process. Examples of these vulnerabilities include:

- Business process/logic or design flaws:
  - Registration forgeries
  - Account/password reset attacks
  - Self-registration and account spoofing
  - Administrative/control channel monitoring and capture
- Development errors:
  - Input validation
  - Parameter processing

  - Authentication bypass
  - Script injection
  - Privilege escalation
- Configuration flaws:
  - Default accounts
  - Accessible administrative interfaces
  - Versioning/error messages
  - Unpatched services
  - Provider/peer relationship forgery
  - Open service abuse
  - Internal/shared configurations

During the exploitation phase, the penetration tester determines whether vulnerabilities can be exploited in order to gain unauthorized access to systems and/or data. The nature of this phase is largely dependent on the findings from the vulnerability discovery phase and must be conducted in accordance with the established Rules of Engagement.

During the information discovery and exploitation phases of the penetration test, testers should maintain the Penetration Test Findings document (IT Security Forms and Aids) to provide a record and accounting of the specific actions taken during the test for use in the final report.

Note: System Owners should be allowed view access to the Penetration Test Findings document during the Penetration Test Exercise but will not be authorized to remediate any of the penetration test findings until after the test window ends as defined in the Authorization Memorandum.

Finally, in the documentation phase, the lead penetration tester will use the Penetration Test Findings document to populate the “Summary of findings” and “Detailed Findings” section of the Penetration Test Report Template (IT Security Forms and Aids). The report will also include a summary indicating the tests conducted, the findings, a severity rating based on the risk to GSA and its interests and related recommendations for mitigation or a technical solution.

Any security issues that are found during the exercise(s) will be presented to the System Owner, together with an assessment of the impact, a proposal for mitigation, or a technical solution.

4.6 Additional Considerations

Tester(s) may leverage tools and techniques that are employed by real attackers, including open source, custom-developed and commercial software tools.t.

All penetration test exercises should be focused on identifying exploitable vulnerabilities in a manner that, if possible, does not affect end-users. The penetration testing team should make every attempt to provide specific windows of time (e.g., maintenance windows) to avoid disruption of system usage by customers.

As the act of trying to penetrate an information system is taking advantage of vulnerabilities in that system this can cause system instability to occur. These instabilities can result in the corruption or loss of data as well as unintentional Denial of Service (DoS). DoS testing is not currently authorized by the GSA. However, if a DoS testing exercise is required; the OSICO IST Division will coordinate with the appropriate GSA Officials for approval.

5 Incident Response Procedures

If a reportable threat or incident is found consistent with the current CIO-IT Security-01-02, the Penetration Testing Team shall stop testing immediately and report the incident to the ISSO, ISSM, and System Owner. Testing will resume after the incident is resolved with the approval of the ISSO, ISSM, and System Owner.

6 Points of Contact

All penetration test exercises must be coordinated through the GSA OCISO. Penetration tests of internal GSA systems (inside the GSA firewall) must also be coordinated with the GSA Penetration Testing Team [iso-pentest@gsa.gov] and GSA Incident Response [gsa-ir@gsa.gov].

Appendix A: Pentest Minimum Requirements Matrix

Table A-1: Pentest Minimum Requirements Matrix

FIPS Level	A&A	Annual Pen Test	Network Pen Test	Delta Pen Test	IR Pen Test
Low	External Interfaces OWASPv4.1 & PTES-TG Gray Box Authenticated	External Interfaces OWASPv4.1 & PTES-TG Gray Box Unauthenticated	External Interfaces	ISSM or CISO Approval External Interfaces	Director or CISO requested. Based on Incident Response SAN's Top 25 and/or PTES-TG
Moderate	External Interfaces OWASPv4.1 & PTES-TG Gray Box Authenticated	External Interfaces OWASPv4.1 & PTES-TG Gray Box Unauthenticated	External Interfaces	ISSM or CISO Approval External Interfaces	Director or CISO requested. Based on Incident Response SAN's Top 25 and/or PTES-TG
High	Internal & External Interfaces OWASPv4.1 & PTES-TG Gray Box Authenticated	Internal and External Interfaces OWASPv4.1 & PTES-TG Gray Box Authenticated	Internal and External Interfaces	ISSM or CISO Approval External Interfaces	Director or CISO requested. Based on Incident Response SAN's Top 25 and/or PTES-TG

Appendix B: Conducting Penetration Test Templates

The following templates are used in the process of conducting penetration tests at GSA. They are available on the GSA InSite IT Security Forms and Aids webpage.

Note: Google Doc versions of the Penetration Testing template are available for internal team penetration tests on Google Drive.

- Kickoff Meeting Presentation Template - documents the appropriate contact information, and establishes key points of the project timeline.
- Penetration Test Rules of Engagement Template - a required agreement that outlines the responsibilities and limitations of the testing team and the system owner throughout the entire testing process. The document must be reviewed and approved by the OCISO IST Division prior to any penetration test exercises.
- Authorization Memorandum Template – prepared by the OCISO IST Division and is a mandatory requirement which (when approved in conjunction with the Rules of Engagement Template), grants authorization to specific members in the Penetration Testing Team to conduct vulnerability assessments and penetration testing against GSA assets.
- Penetration Test Findings Template - documents the security weaknesses found during the penetration test and their origins through the entirety of the process.

Appendix C: GSA A&A Penetration Test Detailed Minimum Requirements

- Web Application Penetration Testing must follow OWASPv4.1 Guidelines
    - No Scenarios, all OWASPv4.1 controls must be tested against. Applicable vs not applicable should be noted in the penetration test documentation.
- Network Penetration Testing must follow PTES-TG guidelines
    - No Scenarios, all PTES-TG controls must be tested against. Applicable vs not applicable should be noted in the penetration test documentation.
- Penetration Tests
    - External facing components must have penetration testing performed from an external perspective.
    - Only components with internal facing only interfaces can be penetration tested from an internal perspective
    - Only Production or Pre-production environments.
    - If authentication is available the pentester must perform the penetration test utilizing authentication.
    - Gray Box Penetration Testing is GSA’s accepted standard.
- Reporting
    - Initial raw scan data should be retained and presented with the final report
    - Final Report Package should include documentation of all OWASPv4.1 controls tested.
    - Final Report should include a screenshot of each finding
    - Final report should include finding Severity
    - Final report should include tool(s) used to identify finding
    - Final report should include a description of each finding.
    - Final report should include all findings before remediation.
        - Remediation can only occur after the file report has been distributed to IST management.
        - Once a finding is remediated the final report should be updated identifying the finding as remediated.
            - The original finding should not be removed from the report
        - False Positive findings should be identified as false positives and not removed from the final report.
            - False Positive findings should include justification for the false positive reclassification.
                - False positive findings are subject to approval from GSA IST and ISO management with final approval from GSA CISO.
    - Each updated final report should be identified by indicating an updated version to the back of the report. (example 02 Penetration Test Report v1.0, 02 Penetration Test Report v1.1, and so on)
- Validations

  - Once a finding is remediated. The systems owner/ISSO/ISSM/or appointed contact should contact the Pentest team for validation. During the assessment period the Pentest team will update the Pentest Report.
    - Once the assessment period is complete, an email will be sent confirming validation. Any further updates will need to be updated in the system's Plan of Action and Milestones (POA&M).